BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-296280

(43)Date of publication of application : 17.10.2003

(51)Int.Cl. G06F 15/00
G09C 1/00
H04L 9/32

(21)Application number : 2002-096995

(22)Date of filing : 29.03.2002

(71)Applicant : HITACHI KOUKIYOU SYST ENG KK

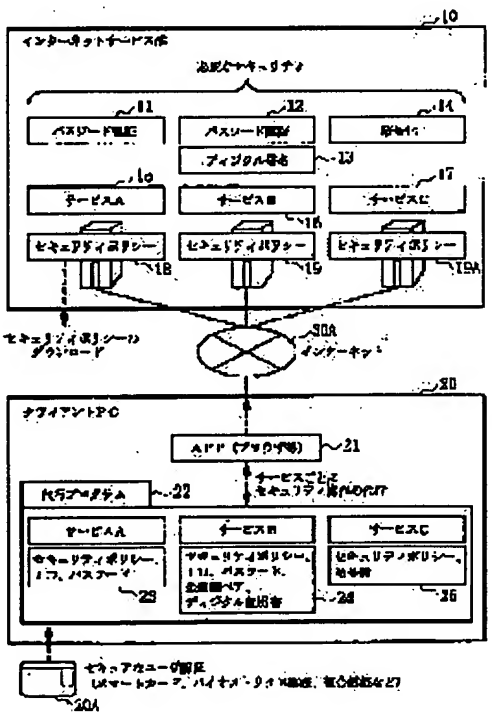
(72)Inventor : MIZUNO TAKASHI
MAEDA HIDEYUKI

(54) SECURITY MEDIATING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To improve usability and to manage security information safely by allowing a general user to only perform the same operation at any time even when using a different service.

SOLUTION: An acting program 22 which performs security management is incorporated in a client PC 20 and security policies are downloaded by services to absorb differences of the policies. The general user combines a smart card for high-safety authentication, biological authentication, or a plurality of authenticating methods and then the acting program carries out necessary security processes such as ciphering 14, password inputs 11 and 12, electronic signing 13 for all services instead. Further, a security policy is distributed from a server to the client and the acting program guides or forces the setting of a proper password, alteration of the password, key update, acquisition of a certificate, etc.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

JP2003-296280

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is the security vicarious execution approach for performing vicarious execution processing which performs a security management to the computer of a client. A smart card, biometrics, or user authentication by compound of two or more authentication approaches is performed. After this user authentication is successful, the security processing vicarious execution program which absorbs the difference in a security policy is started, and the selected service is accessed. By the security processing vicarious execution program Download a security policy from the server of service and a security policy is checked. The security processing vicarious execution approach characterized for a setup with the need for modification by the guide or inputting automatically and a security vicarious execution program performing required security processing of service automatically.

[Translation done.]

JP 2003-296280

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention absorbs the difference in the security policy for every service, and relates to the security vicarious execution approach which can simplify a user's procedure.
[0002]
[Description of the Prior Art] Since the significance of security changes with differences in service when using conventionally the service offered on the Internet, the security policy which is different with each service is needed. Specifically, the authentication approach, a code use plan, and a key management plan will differ from password reinforcement etc. Therefore, different actuation for every service and storage of an item are required of the general user who receives service, and the burden of the present condition is large.
[0003] Moreover, although Cookie was used in many cases in order to realize seamless authentication covering two or more services from before, depending on the configuration of service, the problem might be in security. That is, since Cookie specified the user when it was used as structure for identifying the user to whom the Web server has accessed the site, and it was accessed first, and the both sides of the web browser of a Web server and a user saved this and the same user as a degree accessed the same site, it customized the screen, for example and had how to use [show / a screen with each only for users]. However, when the computer which a user uses changes, the information on Cookie has the problem of becoming an invalid. There was also a problem that use of Cookie will be transmitted from a security hole etc. to the information which should be essentially transmitted by the basis and which does not come out.
[0004] Thus, since a security policy changes with services, a user may carry a smart card and may use a security policy properly with the combination of a password etc. The smart card makes the information on an account required for electronic banking, and information required for individual authentication memorize, and is used as a means of the personal authentication at the time of using a computer and a network.
[0005]
[Problem(s) to be Solved by the Invention] Thus, since a security policy changed with differences in service in using services various in the Internet top conventionally, the user always had to take into consideration password being authentication, password being authentication, whether a digital signature is also required, or encryption would be required each time, and was very troublesome.
[0006] Then, the purpose of this invention is that what is necessary is just to solve the technical problem of these former, and to perform the always same actuation even when using the service from which the general user differed to offer the security vicarious execution approach that usabiliity can be raised and security information can be managed safely.
[0007]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the security vicarious execution approach of this invention offers the vicarious execution program which performs a security

management to a client side, absorbs the difference in a security policy for every service, and simplifies the procedure of the security asked for a general user. Moreover, when a general user performs high authentications (for example, a smart card, vocal-cords authentication, or compound of two or more authentication approaches etc.) of whenever [insurance], a vicarious execution program executes required security processings (for example, encryption, a password input, electronic signature, etc.) of all services by proxy, and they are performed. Moreover, with each service, a security policy is distributed from a server to a client, and the processings (for example, a setup of a suitable password, modification of a password, renewal of a key, acquisition of a certificate, etc.) which need a vicarious execution program are guided, or coercion is exerted. And a program manages the security information of these passwords, a certificate, etc. safely.

[0008] Although a general user's authentication will be unified if a vicarious execution program is used, the whole security will be pulled by the degree of the security of the unified authentication in this. Therefore, in this invention, high authentications (for example, compound of a smart card, biometrics, or two or more authentication approaches etc.) of whenever [insurance] are used for authentication of the general user who unified. As compared with the biological information which only he cannot have, if biometrics are in agreement, they will check with him. In order for what is necessary just to be to perform the always same actuation even when using the service from which the general user differed according to this invention, usabiliity improves. Moreover, since security information is safely manageable, a general user's security improves. Moreover, since application of a security policy can be forced by downloading and applying a security policy, a general user's security improves.

[0009]

[Embodiment of the Invention] Hereafter, a drawing explains the example of this invention to a detail. Drawing 1 is the explanatory view of a security vicarious execution program showing the principle of this invention. In drawing 1 , 10 is [Client PC (personal computer) and 30A of the Internet service group and 20] the Internet. Two or more clients PC 20 are connected to the Internet service group 10 through Internet 30A, and the user shows that these services can be used through Internet 30A from PC20.

[0010] Now, as shown in drawing 1 , there shall be services A, B, and C as a service group. The security policy 18 of service A15 needs only the password authentication 11, the security policy 19 of service B16 needs the password authentication 12 and a digital signature 13, and security policy 19A of service C17 needs encryption 14.

[0011] APP(s) (browser etc.)21 and the vicarious execution program 22 are built in a client PC 20. Each element 25 of the security policy corresponding to Service C in each element 24 of the security policy corresponding to Service B in each element 23 of the SEKYURITE policy corresponding to Service A, ID, and a password, ID, a password, a public key pair, and a digital certificate and a cryptographic key is stored in the vicarious execution program 22 again, respectively.

[0012] There are a smart card, biometrics, compound authentication, etc. as secure user authentication 20A. The service which can log in collectively by this is possible. A password can be made to be able to change or it can respond with the combination of a smart card or a password.

[0013] As an example of a security policy, there is a difference between the term of a password, the die length of a password, and character set doubling (for example, number in which an alphabetic character is made to mix) of a password etc., and there is a difference between the term (it is made to change) of a certificate and the term (it is made to change) of a key etc. in a digital signature. When service is mentioned concretely, there are dealings between companies as service A15 of only the password authentication 11. Moreover, there are dealings of stocks as the password authentication 12 and service B16 of a digital signature 13. Moreover, there are dealings with a bank as service C17 of encryption 14.

[0014] Drawing 14 is the operation flow chart of the security vicarious execution approach of this invention. If user authentication is set to O.K. by inserting smart card 20A in PC20, the processing flow of a security processing vicarious execution program will advance in the following order.

(1) Access authentication activation (3) service of security processing vicarious execution program starting (step 101) and (2) security processing vicarious execution program (step 102).

(4) It is [whether a security processing vicarious execution program can be used and] the server of decision (step 103) and (5) services to a security policy Download (step 104) and [0015] (6) It will be made to set up if there is a setup which must make a processing continuation (6-2) change without doing anything if there is no setup which must make a check (6-1) change of the security policy (for example, since the password has expired). It will be made to set up if the need (step 105,106) and a setup which must be set up newly (6-3) have resetting of a password (step 105,106). (for example, since the first service was accessed, a setup of ID and a password need)
[0016] (7) Access security processing required for service again at automatic activation (step 107) and the Internet [step 102] without return and security.
(8) if required security processing is completed -- usually -- a passage -- service -- use and (9) -- also using another service as it is -- the possibility of and [0017] As a result of downloading, when modification of a security policy is the need, it directs about it. That is, since there is also usually a user who is not looking at it although a change notice is performed in the location of a homepage or others when a security policy has modification about Services A, B, and C and ..., it directs here. After performing the input corresponding to the changed policy, it moves to security processing. The usual processing is performed after it.
[0018] Drawing 2 - drawing 13 are the transition diagrams on the screen in the case of carrying out this invention. Drawing 2 is the screen Fig. of a log in in a security processing vicarious execution program. First, by Screen 30 of drawing 2 being displayed, it turns out that a security processing vicarious execution program processes, and a user inserts IC cards (smart card etc.) according to directions of "insert an IC card."
[0019] Drawing 3 is the screen Fig. of a log in in a security processing vicarious execution program. Since Screen 31 of drawing 3 is displayed by inserting an IC card, a user enters a password into the input column according to directions of "enter a password."
[0020] Drawing 4 is the screen Fig. of a security processing vicarious execution program authentication success. Screen 32 of drawing 4 is displayed as a result of an input of a password. it succeeded in "authentication! " -- " -- all of the security processing to which it corresponds [subsequent] are executed by proxy -- " -- ** -- since it is displayed, a user knows that it is necessary to carry out no actuation henceforth.
[0021] Drawing 5 is the screen Fig. of new service use initiation. Next, it being "Ox bank online banking" and the thing "for which this service supports the security processing vicarious execution program" are displayed by specifying bank relation. And even if a user operates nothing, the actuation which the current line of a security vicarious execution program requires is displayed down Screen 33. Current is displayed "To check a security policy."
[0022] Drawing 6 is the screen Fig. of security policy download. the lower part of after the check of a security policy, and this screen 34 -- "security policy -- under download -- " -- a display is issued.
[0023] Drawing 7 is the screen Fig. of a check of a security policy. Although authentication is immediately performed by performing the input corresponding to the condition when there is no modification of a security policy, the case where there is modification of a policy here is shown. The term of this password is specified in one month by "security policy as a result of the check. since the password expired, please set up newly -- " -- a display is made. By this, a user will enter a new password into the input column. In reinput, it inputs at the reinput column. "Under security setting activation" is displayed down Screen 35 now.
[0024] Drawing 8 is the screen Fig. of a security setup of new service. the result of a security policy check -- " -- ID and a password need to be set up to use this service. Please set up. Since the display which is " was issued, a user enters ID into the ID input column of Screen 36, and enters a password into the password input column, respectively. When there is the need for reinput, it inputs into the reinput column. "Under new security setting activation" is displayed down Screen 36.
[0025] Drawing 9 is a screen Fig. which carries out automatic activation of the authentication of service. By setting up a password, or ID and a password, a security vicarious execution program performs authentication of service automatically. "Under authentication activation" is displayed down Screen 37.

[0026] Drawing 10 is the screen Fig. of a log in success to service. A success of authentication performs a log in in Ox bank in service and this case. It is displayed as "Mr. ****'s account menu", and the screen which chooses account balance authentication, transfer, a log out, and either is displayed. Moreover, down Screen 38, it indicates "it carried out an authentication success."
[0027] Drawing 11 is a screen Fig. in use of another service of this invention. Here, download of the security policy in the case of a stock dealing is **********. the display of "uneven security online" and "this service supporting the security processing vicarious execution program" should do to Screen 39 -- the lower part of a screen -- "security policy -- under download -- " -- it is displayed.
[0028] Drawing 12 is a screen Fig. which carries out automatic activation of the authentication following the screen of drawing 11 . After a security processing vicarious execution program downloads a security policy automatically by drawing 11 , automatic activation of authentication is performed by this screen 40. "Under authentication automatic activation" is displayed down Screen 40.
[0029] Drawing 13 is a screen Fig. when authentication is successful following the screen of drawing 12 . When authentication is successful, Mr. ****'s exclusive page is displayed and the screen to which selection of an account check and investment service is urged is displayed. Down Screen 41, it indicates "it carried out an authentication success." After this, the dealings which checked the account to see the user consulted about investment, or met one of the purposes are conducted.
[0030] The processing flow of the security processing vicarious execution program shown in drawing 14 is changed into a program, and by storing the program which changed in record media, such as CD-ROM, PC of arbitration is equipped with a record medium, and if a program is installed in PC and performed, security processing vicarious execution of this invention can be realized easily.
[0031]
[Effect of the Invention] In order for what is necessary just to be to perform the always same actuation even when using the service from which the general user differed according to this invention, as explained above, it is effective in usabiliity improving. Moreover, it is possible to manage security information safely, and since application of a security policy is forced by downloading and applying a security policy, a general user's security is effective in improving.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－296280
（P2003－296280A）
(43)公開日　平成15年10月17日(2003.10.17)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ	５Ｂ０８５
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｅ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ	

審査請求　未請求　請求項の数１　ＯＬ　（全 11 頁）

(21)出願番号　特願2002－96995(P2002－96995)

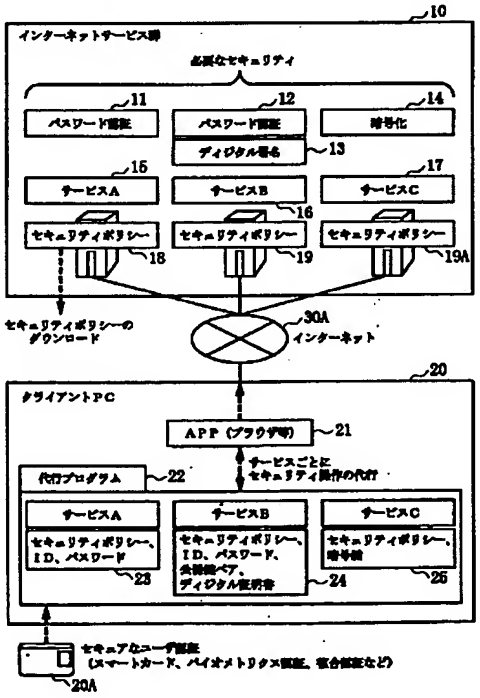
(22)出願日　平成14年３月29日(2002.3.29)

(71)出願人　596127554
日立公共システムエンジニアリング株式会社
東京都江東区東陽２丁目４番18号
(72)発明者　水野　高志
東京都江東区東陽２丁目４番18号　日立公共システムエンジニアリング株式会社内
(72)発明者　前田　英行
東京都江東区東陽２丁目４番18号　日立公共システムエンジニアリング株式会社内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

最終頁に続く

(54)【発明の名称】　セキュリティ代行方法

(57)【要約】
【課題】一般ユーザが異なったサービスを利用する場合でも、常に同じ操作を行うだけでよく、ユーザビリティを向上させ、かつセキュリティ情報を安全に管理することができる。
【解決手段】クライアントＰＣ２０にセキュリティ管理を行う代行プログラム２２を内蔵し、サービスごとにセキュリティポリシーをダウンロードすることで、ポリシーの違いを吸収する。一般ユーザは安全度の高い認証のスマートカード、生体認証または複数の認証方法の複合等を行うことにより、全てのサービスの必要なセキュリティ処理、暗号化１４、パスワード入力１１，１２、電子署名１３等を代行プログラムが代行して行う。また、セキュリティポリシーをサーバからクライアントへ配付し、代行プログラムが適切なパスワードの設定、パスワードの変更、鍵更新、証明書の取得等をガイドするか、あるいは強制する。



【特許請求の範囲】
【請求項１】　クライアントのコンピュータにセキュリティ管理を行う代行処理を実行させるためのセキュリティ代行方法であって、
スマートカード、生体認証または複数の認証方法の複合によるユーザ認証を行い、
該ユーザ認証が成功した後、セキュリティポリシーの違いを吸収するセキュリティ処理代行プログラムを起動し、
選択されたサービスにアクセスし、
セキュリティ処理代行プログラムにより、サービスのサーバからセキュリティポリシーをダウンロードし、
セキュリティポリシーを確認して、変更の必要がある設定をガイドまたは自動的に入力し、
サービスの必要なセキュリティ処理をセキュリティ代行プログラムが自動的に実行することを特徴とするセキュリティ処理代行方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、サービスごとのセキュリティポリシーの違いを吸収し、ユーザの手続きを簡単にすることが可能なセキュリティ代行方法に関する。
【０００２】
【従来の技術】従来、インターネット上で提供されるサービスを利用する場合、サービスの違いによってセキュリティの重要度が異なるため、それぞれのサービスで違ったセキュリティポリシーが必要になる。具体的には、認証方法、暗号利用方針、鍵管理方針、パスワード強度などが異なることになる。そのため、サービスを受ける一般ユーザは、サービスごとに異なった操作および項目の記憶を要求され、その負担が大きいのが現状である。
【０００３】また、従来より、複数サービスにわたるシームレスな認証を実現するために、Ｃｏｏｋｉｅが利用されることが多いが、サービスの構成によってはセキュリティに問題があることがあった。すなわち、Ｃｏｏｋｉｅは、Ｗｅｂサーバがサイトにアクセスしてきたユーザを識別するための仕組みとして使われ、最初にアクセスされた際に、Ｗｅｂサーバとユーザのブラウザの双方がこれを保存しておき、次に同じユーザが同じサイトをアクセスした場合に、ユーザを特定できるので、例えば画面をカスタマイズして個々のユーザ専用の画面を見せるなどの使い方があった。しかし、もし、ユーザが使用するコンピュータが変わった場合にはＣｏｏｋｉｅの情報は無効になってしまうという問題がある。セキュリティホールなどから、Ｃｏｏｋｉｅの利用がもとで本来送信すべきでない情報まで送信されてしまう、という問題もあった。
【０００４】このように、サービスによってセキュリティポリシーが異なるため、ユーザは例えば、スマートカードを携帯し、パスワードの組み合わせなどにより、セキュリティポリシーの使い分けを行う場合もある。スマートカードは、電子決済に必要な口座の情報や、個人の認証に必要な情報を記憶させておき、コンピュータやネットワークを利用する際の個人認証の手段として使用される。
【０００５】
【発明が解決しようとする課題】このように、従来、インターネット上で種々のサービスを利用する場合には、サービスの違いによりセキュリティポリシーが異なるため、ユーザはその都度、パスワード認証のみか、パスワード認証とディジタル署名も必要であるか、暗号化が必要であるか等を常時考慮しておかなくてはならず、極めて面倒であった。
【０００６】そこで、本発明の目的は、これら従来の課題を解決し、一般ユーザが異なったサービスを利用する場合でも、常に同じ操作を行うだけでよく、ユーザビリティを向上させ、かつセキュリティ情報を安全に管理することができるセキュリティ代行方法を提供することにある。
【０００７】
【課題を解決するための手段】上記目的を達成するため、本発明のセキュリティ代行方法は、クライアント側にセキュリティ管理を行う代行プログラムを提供し、サービスごとにセキュリティポリシーの違いを吸収して、一般ユーザが求められるセキュリティの手続きを簡略化する。また、一般ユーザが安全度の高い認証（例えば、スマートカード、声帯認証または複数の認証方法の複合等）を行うことにより、全てのサービスの必要なセキュリティ処理（例えば、暗号化、パスワード入力、電子署名等）を代行プログラムが代行して行う。また、それぞれのサービスでは、セキュリティポリシーをサーバからクライアントへ配付し、代行プログラムが必要な処理（例えば、適切なパスワードの設定、パスワードの変更、鍵更新、証明書の取得等）をガイドするか、あるいは強制する。そして、これらパスワード、証明書等のセキュリティ情報を、プログラムが安全に管理する。
【０００８】代行プログラムを利用すると、一般ユーザの認証を統一してしまうことになりがちであるが、これでは、全体のセキュリティは統一した認証のセキュリティの度合いに引張られることになる。そのため、本発明では、統一した一般ユーザの認証には、安全度の高い認証（例えば、スマートカード、生体認証または複数の認証方法の複合等）を用いる。生体認証は、本人しか持ち得ない生体情報と比較して、一致すれば本人と確認するものである。本発明によれば、一般ユーザが異なったサービスを利用する場合でも、常に同じ操作を行うだけでよいため、ユーザビリティが向上する。また、セキュリティ情報を安全に管理することができるため、一般ユーザのセキュリティが向上する。また、セキュリティポリ

シーをダウンロードして適用することにより、セキュリティポリシーの適用を強制することができるため、一般ユーザのセキュリティが向上する。

【0009】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明の原理を示すセキュリティ代行プログラムの説明図である。図1において、10はインターネットサービス群、20はクライアントPC（パーソナルコンピュータ）、30Aはインターネットである。複数のクライアントPC20がインターネット30Aを介してインターネットサービス群10に接続され、ユーザはPC20からインターネット30Aを介してこれらのサービスを利用できることを示している。

【0010】いま、図1に示すように、サービス群としてサービスA，B，Cがあるものとする。サービスA15のセキュリティポリシー18は、パスワード認証11のみを必要とし、サービスB16のセキュリティポリシー19は、パスワード認証12とディジタル署名13を必要とし、サービスC17のセキュリティポリシー19Aは、暗号化14を必要としている。

【0011】クライアントPC20には、APP（ブラウザ等）21、代行プログラム22が内蔵される。代行プログラム22には、サービスAに対応したセキュリテポリシー、ID、パスワードの各要素23が、またサービスBに対応したセキュリティポリシー、ID、パスワード、公開鍵ペア、ディジタル証明書の各要素24が、またサービスCに対応したセキュリティポリシー、暗号鍵の各要素25が、それぞれ格納されている。

【0012】セキュアなユーザ認証20Aとして、スマートカード、生体認証、複合認証などがある。これにより、一括してログインできるようなサービスが可能である。パスワードの変更をさせたり、スマートカードやパスワードの組み合わせにより対応することができる。

【0013】セキュリティポリシーの一例としては、パスワードの期限、パスワードの長さ、パスワードの文字の組合わせ（例えば、文字を混入させる数）の違いなどがあり、ディジタル署名には、証明書の期限（変更させる）およびキーの期限（変更させる）の違いなどがある。サービスを具体的に挙げると、パスワード認証11のみのサービスA15としては、企業間の取引がある。また、パスワード認証12とディジタル署名13のサービスB16としては、株式の取引がある。また、暗号化14のサービスC17としては、銀行との取引がある。

【0014】図14は、本発明のセキュリティ代行方法の動作フローチャートである。スマートカード20AをPC20に挿入することにより、ユーザ認証がOKになると、次の順序でセキュリティ処理代行プログラムの処理フローが進行する。

（1）セキュリティ処理代行プログラム起動（ステップ101）、

（2）セキュリティ処理代行プログラムの認証実行

（3）サービスにアクセス（ステップ102）

（4）セキュリティ処理代行プログラムが利用できるかを判断（ステップ103）、

（5）サービスのサーバからセキュリティポリシーをダウンロード（ステップ104）、

【0015】（6）セキュリティポリシーを確認

（6－1）変更しなければならない設定がなければ、何もしないで処理続行

（6－2）変更しなければならない設定があれば、設定させる（例えば、パスワードの期限が切れているので、パスワードの再設定が必要）（ステップ105，106）、

（6－3）新規に設定しなければならない設定があれば、設定させる（例えば、初めてのサービスにアクセスしたため、IDとパスワードの設定が必要）（ステップ105，106）

【0016】（7）サービスに必要なセキュリティ処理を自動実行（ステップ107）、再度、ステップ102に戻り、セキュリティなしのインターネットにアクセスする。

（8）必要なセキュリティ処理が終了すれば、通常通りサービスを利用、

（9）そのまま別のサービスを利用することも可能、

【0017】ダウンロードした結果、セキュリティポリシーの変更が必要の場合には、それについて指示を行う。すなわち、サービスA，B，C，・・・について、セキュリティポリシーに変更がある場合には、通常、ホームページやその他の場所に変更通知が行われるが、それを見ていないユーザもあるので、ここで指示を行う。変更されたポリシーに合致する入力を行った後、セキュリティ処理に移る。それ以降は、通常の処理を実行する。

【0018】図2～図13は、本発明を実施する場合の画面上の遷移図である。図2は、セキュリティ処理代行プログラムへのログインの画面図である。先ず、図2の画面30が表示されていることで、ユーザはセキュリティ処理代行プログラムが処理することがわかり、『ICカードを挿入してください』の指示に従ってICカード（スマートカード等）を挿入する。

【0019】図3は、セキュリティ処理代行プログラムへのログインの画面図である。ICカードが挿入されることにより、図3の画面31が表示されるので、ユーザは『パスワードを入力してください』の指示に従って、入力欄にパスワードを入力する。

【0020】図4は、セキュリティ処理代行プログラム認証成功の画面図である。パスワードの入力の結果、図4の画面32が表示される。『認証に成功しました！』『以降の対応するセキュリティ処理はすべて代行しま

す』と表示されるので、ユーザは以降は操作を何もしなくてもよいことを知る。

【００２１】図5は、新規サービス利用開始の画面図である。次に、銀行取引を指定することで、『○×銀行オンラインバンキング』であること、および『このサービスはセキュリティ処理代行プログラムに対応している』ことが表示される。そして、ユーザは何も操作しなくても、セキュリティ代行プログラムの現在行っている操作が、画面３３の下方に表示される。現在は、『セキュリティポリシーをチェックします』と表示される。

【００２２】図6は、セキュリティポリシーダウンロードの画面図である。セキュリティポリシーのチェックの後、この画面３４の下方には『セキュリティポリシーをダウンロード中』の表示が出される。

【００２３】図7は、セキュリティポリシーの確認の画面図である。セキュリティポリシーの変更がない場合には、その条件に合致した入力を行うことで直ちに認証が行われるが、ここではポリシーの変更があった場合が示されている。確認の結果、『セキュリティポリシーによって、このパスワードの期限は１ケ月に指定されています。パスワードの期限が切れたので新しく設定して下さい』の表示がなされる。これにより、ユーザは新パスワードを入力欄に入力することになる。再入力の場合には、再入力欄に入力する。画面３５の下方には、現在『セキュリティ設定実行中』が表示されている。

【００２４】図8は、新規サービスのセキュリティ設定の画面図である。セキュリティポリシー確認の結果、『このサービスを利用するにはＩＤとパスワードの設定が必要です。設定してください。』の表示が出されたので、ユーザは画面３６のＩＤ入力欄にＩＤを、パスワード入力欄にパスワードを、それぞれ入力する。再入力の必要がある場合には、再入力欄に入力する。画面３６の下方には、『新規セキュリティ設定実行中』が表示されている。

【００２５】図9は、サービスの認証を自動実行する画面図である。パスワードまたはＩＤとパスワードを設定することにより、サービスの認証をセキュリティ代行プログラムが自動的に実行する。画面３７の下方には、『認証実行中』が表示される。

【００２６】図１０は、サービスへのログイン成功の画面図である。認証が成功すると、サービス、この場合には○×銀行へのログインが行われる。『□△さんの口座メニュー』と表示され、口座残高認証か、振り込みか、ログアウトか、いずれかを選択する画面が表示される。また、画面３８の下方には、『認証成功しました』が表示されている。

【００２７】図１１は、本発明の別のサービスの利用の場合の画面図である。ここでは、株式取引の場合のセキュリティポリシーのダウンロードが行われている。画面３９には、『凸凹証券オンライン』『このサービスはセキュリティ処理代行プログラムに対応しています』の表示がなされ、画面の下方には、『セキュリティポリシーをダウンロード中』が表示される。

【００２８】図１２は、図１１の画面に続き、認証を自動実行する画面図である。図１１でセキュリティ処理代行プログラムが自動的にセキュリティポリシーをダウンロードした後、この画面４０によって認証の自動実行が行われる。画面４０の下方には、『認証自動実行中』が表示される。

【００２９】図１３は、図１２の画面に続き、認証が成功した場合の画面図である。認証が成功することにより、□△さんの専用ページが表示され、口座確認か、投資サービスかの選択を促す画面が表示される。画面４１の下方には『認証成功しました』が表示される。これ以降は、ユーザが投資の相談をするか、口座を確認するか、いずれかの目的に沿った取引が行われる。

【００３０】図１４に示すセキュリティ処理代行プログラムの処理フローをプログラムに変換し、変換したプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておくことで、任意のＰＣに記録媒体を装着し、プログラムをＰＣにインストールして実行させれば、本発明のセキュリティ処理代行が容易に実現できる。

【００３１】

【発明の効果】以上説明したように、本発明によれば、一般ユーザが異なったサービスを利用する場合でも、常に同じ操作を行うだけでよいため、ユーザビリティが向上するという効果がある。また、セキュリティ情報を安全に管理することが可能であり、またセキュリティポリシーをダウンロードして適用することにより、セキュリティポリシーの適用を強制するので、一般ユーザのセキュリティは向上するという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例を示すセキュリティ処理代行プログラムの概略説明図である。

【図２】本発明のセキュリティ処理代行プログラムへのログイン画面図（１）である。

【図３】本発明のセキュリティ処理代行プログラムへのログイン画面図（２）である。

【図４】本発明のセキュリティ処理代行プログラム認証成功の画面図である。

【図５】本発明の新規サービス利用開始の画面図である。

【図６】本発明のセキュリティポリシーダウンロードの画面図である。

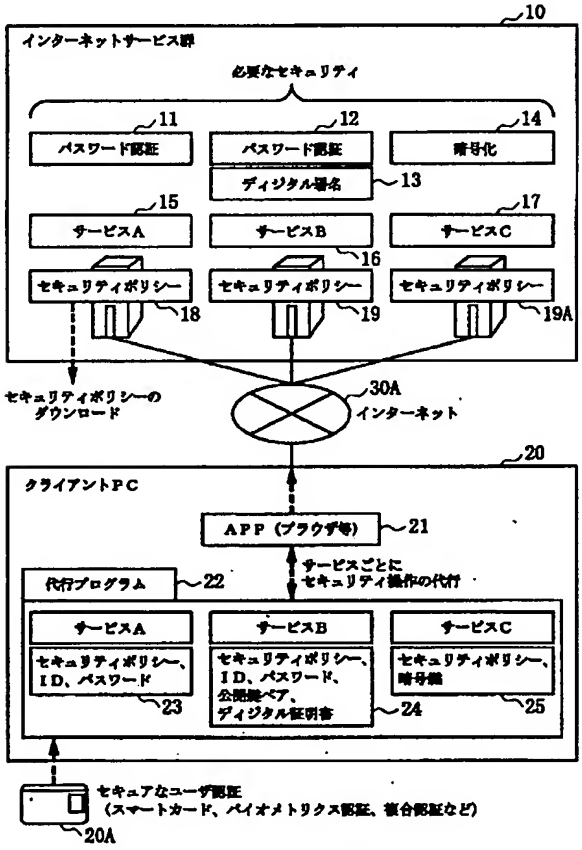
【図７】本発明のセキュリティポリシーの確認画面図である。

【図８】本発明の新規サービスのセキュリティ設定画面図である。

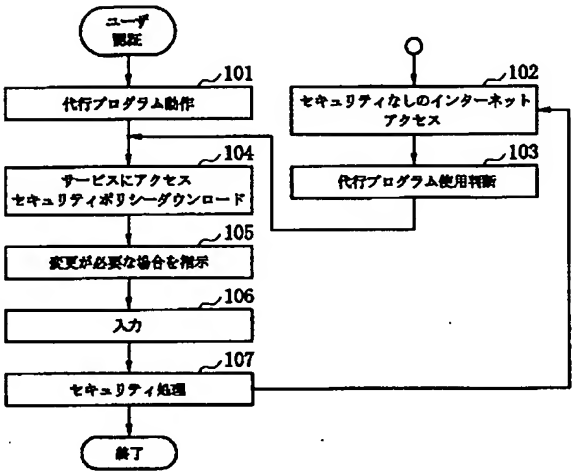
【図９】本発明のサービスの認証を自動実行する画面図である。

【図１０】本発明のサービスへのログイン成功の画面図である。
【図１１】本発明の別のサービスの利用画面図である。
【図１２】本発明の別のサービスの認証を自動実行する画面図である。
【図１３】本発明の別のサービスへのログインの画面図である。
【図１４】本発明の一実施例を示すセキュリティ処理代行プログラムの動作フローチャートである。
【符号の説明】
１０…インターネットサービス群、１１，１２…パスワード認証、１４…暗号化、１３…ディジタル署名、１５…サービスＡ、１６…サービスＢ、１７…サービスＣ、１８，１９，１９Ａ…セキュリティポリシー、３０Ａ…インターネット、２０…クライアントＰＣ、２１…ＡＰＰ（ブラウザ等）、２２…セキュリティ処理代行プログラム、２３…サービスＡのセキュリティ要素群、２４…サービスＢのセキュリティ要素群、２５…サービスＣのセキュリティ要素群、２０Ａ…ユーザ認証媒体。

【図１】

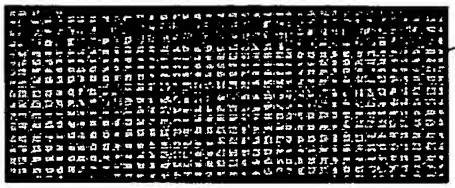


【図１４】



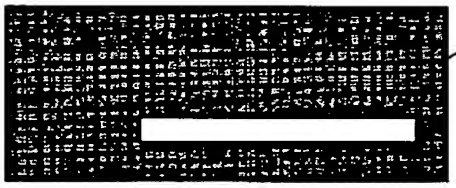
【図2】

①セキュリティ処理代行プログ
ラムへログイン　－ ICカード



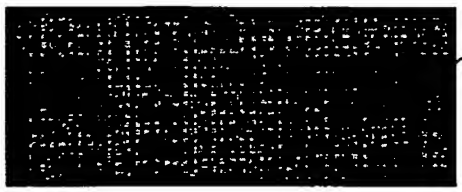
【図3】

②セキュリティ処理代行プログ
ラムへログイン　－ パスワード



【図4】

③セキュリティ処理代行プログ
ラム認証成功

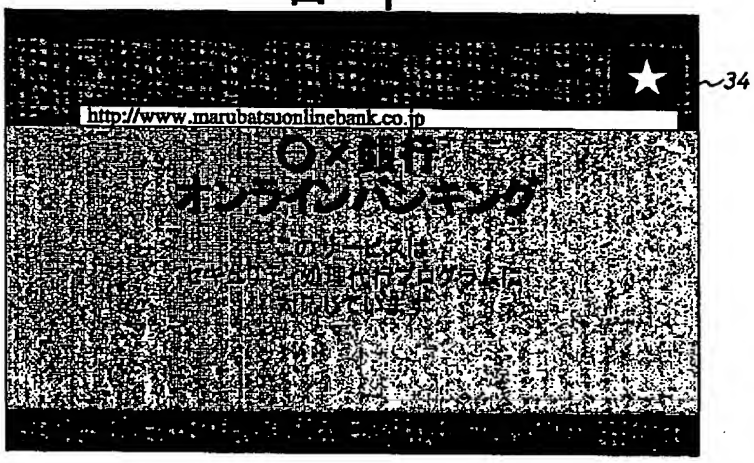


【図5】

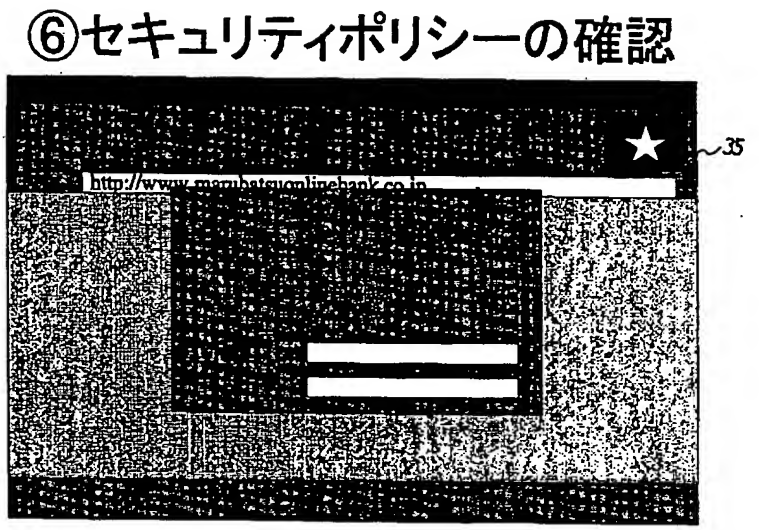
④新規サービス利用開始

【図6】

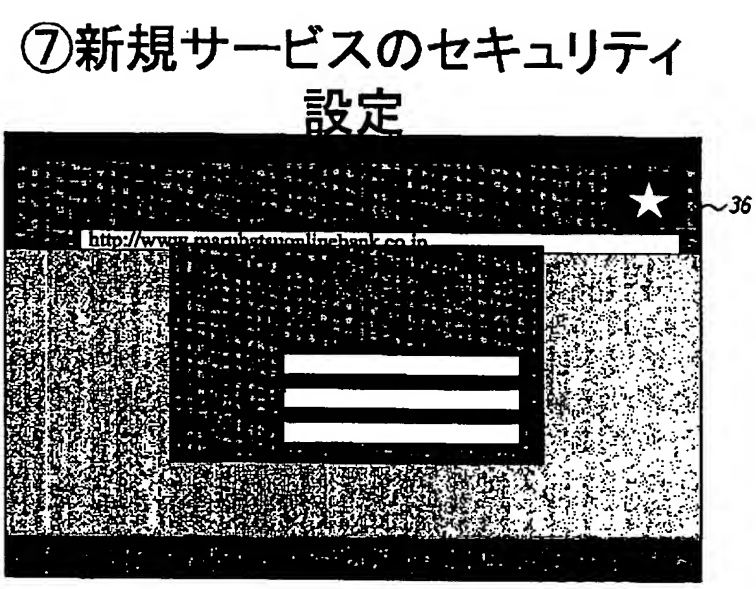
⑤セキュリティポリシーダウンロード



【図7】

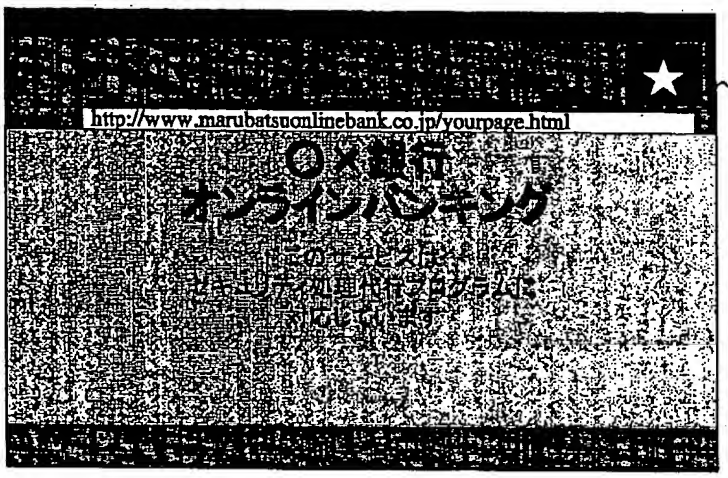


【図8】



【図9】

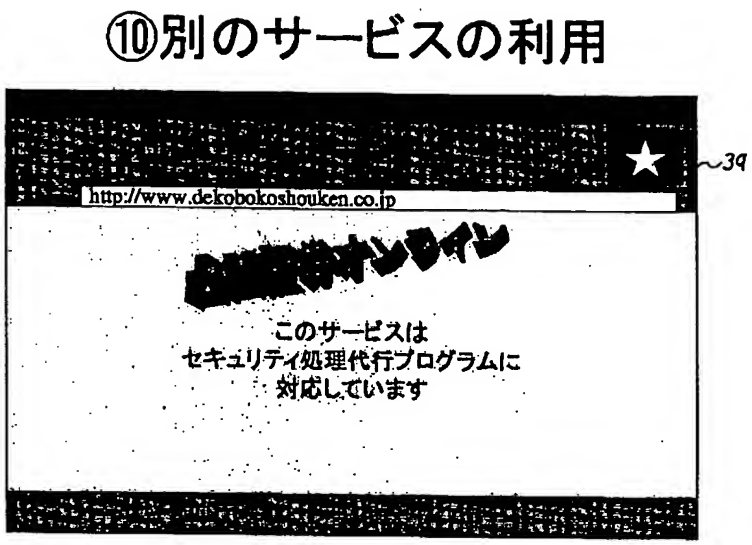
⑧サービスの認証を自動実行



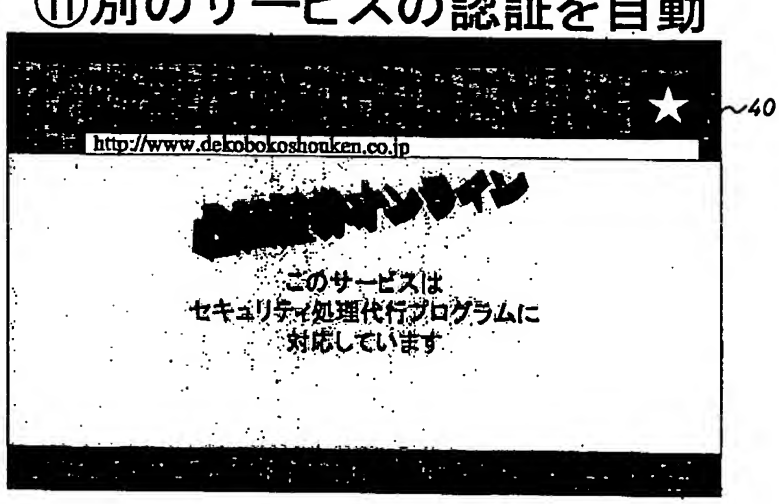
【図10】

⑨サービスへのログイン成功

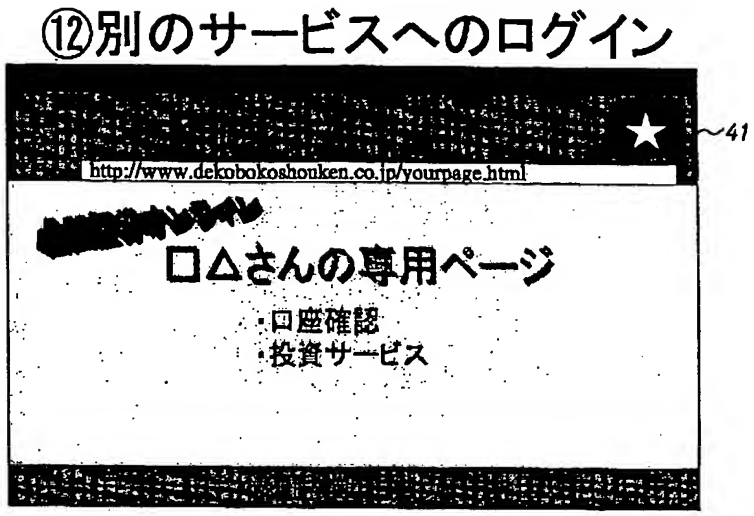
【図11】


⑩別のサービスの利用
http://www.dekobokoshouken.co.jp
このサービスは
セキュリティ処理代行プログラムに
対応しています
39

【図12】


⑪別のサービスの認証を自動
http://www.dekobokoshouken.co.jp
このサービスは
セキュリティ処理代行プログラムに
対応しています
40

【図13】



フロントページの続き

Fターム(参考) 5B085 AE02 AE06 AE12 AE25
5J104 AA07 KA01 KA16 NA05